CLAIMS

1. A method comprising:

presenting a user with a plurality of modes of operation, wherein the plurality of modes of operation define different trust options for handling sensitive data associated with the user;

receiving a selection from the user, wherein the selection is one of the plurality of modes of operation; and

handling sensitive data associated with the user in accordance with the selected mode of operation.

2. A method as recited in claim 1 wherein the plurality of modes include a low trust option for handling sensitive data associated with the user, the low trust option configured to retrieve sensitive data from the user each time the user requests a service requiring the sensitive data.

3. A method as recited in claim 2 wherein the low trust option does not persistently store sensitive data after the requested service requiring the sensitive data has been completed.

4. A method as recited in claim 1 wherein the plurality of modes include a high trust option for handling sensitive data associated with the user, the high trust option configured to retrieve sensitive data from the user and store the sensitive data in an encrypted format for future use.

5. A method as recited in claim 1 wherein the plurality of modes include a high trust option for handling sensitive data associated with the user, the high trust option configured to retrieve sensitive data from the user, encode the sensitive data using a two-way encryption technique, and store the encrypted sensitive data.

6. A method as recited in claim 1 wherein the plurality of modes include a moderate trust option for handling sensitive data associated with the user, the moderate trust option configured to retrieve sensitive data from the user and store the sensitive data in an encrypted format using a password known only to the user.

7. A method as recited in claim 1 wherein the plurality of modes include a moderate trust option for handling sensitive data associated with the user, the moderate trust option configured to retrieve sensitive data from the user, encode the sensitive data using a one-way encryption technique, and store the encrypted sensitive data.

8. A method as recited in claim 1 further comprising assigning a default mode of operation if the user does not select a valid mode of operation.

9. A method as recited in claim 1 further comprising associating a user account with the selected mode of operation.

10. A method comprising:

presenting a user with a low trust mode of operation, wherein the low trust mode of operation retrieves sensitive data from the user each time the user requests a service requiring the sensitive data;

presenting the user with a high trust mode of operation, wherein the high trust mode of operation stores sensitive data received from the user in an encrypted format;

receiving a selection from the user indicating one of the two modes of operation; and

handling sensitive data associated with the user in accordance with the selected mode of operation.

11. A method as recited in claim 10 further comprising presenting the user with a moderate trust mode of operation, wherein the moderate trust mode of operation stores sensitive data from the user in an encrypted format using a password known to the user; and wherein receiving a selection from the user includes receiving a selection indicating one of the three modes of operation.

12. A method as recited in claim 10 further comprising associating a user account with the selected mode of operation.

13. A method as recited in claim 10 further comprising assigning a default trust mode if the user does not select a valid mode of operation.

14. One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 10.

15. A method comprising:

presenting a user with a moderate trust mode of operation, wherein the moderate trust mode of operation stores sensitive data from the user in an encrypted format using a password known to the user;

presenting the user with a high trust mode of operation, wherein the high trust mode of operation stores sensitive data received from the user;

receiving a selection from the user indicating one of the two modes of operation; and

handling sensitive data associated with the user in accordance with the selected mode of operation.

16. One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 15.

17. A method comprising:

presenting a user with a moderate trust mode of operation, wherein the moderate trust mode of operation stores sensitive data from the user in an encrypted format using a password known to the user;

presenting the user with a low trust mode of operation, wherein the low trust mode of operation retrieves sensitive data from the user each time the user requests a service requiring the sensitive data;

receiving a selection from the user indicating one of the two modes of operation; and

handling sensitive data associated with the user in accordance with the selected mode of operation.

18. One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 17.

19. One or more computer-readable media having stored thereon a computer program that, when executed by one or more processors, causes the one or more processors to:

present a user with a plurality of modes of operation, wherein the plurality of modes of operation define different trust options for handling sensitive data associated with the user;

receive a selection from the user, wherein the selection is one of the plurality of modes of operation; and

process sensitive data associated with the user in accordance with the selected mode of operation.

20. One or more computer-readable media as recited in claim 19 wherein the plurality of modes of operation include a low trust option for handling sensitive data associated with the user, the low trust option configured to retrieve sensitive data from the user each time the user requests a service requiring the sensitive data.

21. One or more computer-readable media as recited in claim 20 wherein the low trust option does not persistently store sensitive data after the requested service requiring the sensitive data is complete.

22. One or more computer-readable media as recited in claim 19 wherein the plurality of modes of operation include a high trust option for handling sensitive data associated with the user, the high trust option configured to retrieve sensitive data from the user and store the sensitive data in an encrypted format.

23. One or more computer-readable media as recited in claim 19 wherein the plurality of modes of operation include a moderate trust option for handling sensitive data associated with the user, the moderate trust option configured to retrieve sensitive data from the user and store the sensitive data in an encrypted format using a password known only to the user.